Naval War College
Newport, R.I.

# The Vulnerabilities of US Strategic Ports to Acts of Sabotage

By

David C. Grohoski
MAJ, USA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Maritime Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature David C. Grohoski.

12 February 1996

Paper Directed By
David D. Watson, Captain, USN
Chairman, Joint Military Operations Department



CAPT Charles C. Beck
Faculty Advisor

9 Feb 96
Date

**REPORT DOCUMENTATION PAGE**

| | |
|---|---|
| **1. Report Security Classification:** Unclassified | |
| **2. Security Classification Authority:** | |
| **3. Declassification/Downgrading Schedule:** | |
| **4. Distribution/Availability of Report:** Distribution statement A: Approved for public release; Distribution is unlimited. | |
| **5. Name of Performing Organization:** Joint Military Operations Dept. | |
| **6. Office Symbol:** NWC Code 1C | **7. Address:** Naval War College<br>686 Cushing Road<br>Newport, RI 02841-1207 |
| **8. Title:** The Vulnerabilities of U.S. Strategic Ports to Sabotage (U) ^Acts of | |
| **9. Personal Authors:** MAJ David C. Grohoski, USA | |
| **10.Type of Report:** Final | **11. Date of Report:** 12 February 1996 |
| **12.Page Count:** ~~36~~ | |
| **13.Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | |
| **14. Ten key words that relate to your paper:** Port Security, Terrorism, Sabotage, Terminal Security, Port Vulnerabilities, Sealift Vulnerabilities | |

**15.Abstract:** In an era where war is a "come as you are" affair, the ramifications of arriving too late, or with insufficient forces could prove to be devastating. The recent bombings of the World Trade Center and in Oklahoma City shattered the myth that the United States is exempt from the effects of terrorism. The changing global security environment demands increase vigilance in guarding our vital institutions. The U.S. deterrent policy relies on power projection and the ability to get forces to areas of crisis in a timely manner. The U.S. deploys 95% of its supplies and equipment by sea. We can no longer assume that our domestic seaports are free from the effects of sabotage and terrorism. The U.S. seaports present an exposed target whose attack would serve to enhance the aims of any terrorist organization. It is conceivable that a single, violent act could shatter the balanced, time-sensitive U.S. deployment schedule. The vulnerabilities of our strategic seaports, which deploy and sustain our forces, demands a new sense of awareness on the part of the Department of Defense.

| **16.Distribution/ Availability of Abstract:** | **Unclassified** | **Same As Rpt** | **DTIC Users** |
|---|---|---|---|
| | X | | |
| **17.Abstract Security Classification:** Unclassified | | | |
| **18.Name of Responsible Individual:** Chairman, Joint Military Operations Department | | | |
| **19.Telephone:** 841-~~6461~~ 6461 | **20.Office Symbol:** NWC Code 1C | | |

Abstract of

The Vulnerabilities of US Strategic Ports to Acts of Sabotage

In an era where war is a "come as you are" affair, the ramifications of arriving too late, or with insufficient forces could prove to be devastating. The recent bombings of the World Trade Center and in Oklahoma City shattered the myth that the United States is exempt from the effects of terrorism. The changing global security environment demands increased vigilance in guarding our vital institutions. The US deterrent policy relies on power projection and the ability to get forces to areas of crisis in a timely manner. The US deploys 95% of its supplies and equipment by sea. We can no longer assume that our domestic seaports are free from the effects of sabotage and terrorism. The US seaports present an exposed target whose attack would serve to enhance the aims of any terrorist organization. It is conceivable that a single, violent act could shatter the balanced, time-sensitive US deployment schedule. The vulnerabilities of our strategic seaports, which deploy and sustain our forces, demands a new sense of awareness on the part of the Department of Defense.

## Table of Contents

## Introduction

Ports have played a vital role in the defense of our nation from our colonial beginnings to the recent war in Iraq. With the cessation of the Cold War and lessons learned in Operations Desert Shield, Desert Storm, Restore Hope, Vigilant Warrior and other operations, the ports' role has proven to be a vital aspect of our national defense.

Among the challenges facing the Department of Defense (DoD) is the underestimation of specific vulnerabilities to the continental United States (CONUS) Theater of Operations. DoD has tended to focus on the out-of-OCONUS (OCONUS) theater threat and to neglect the operational aspects of a CONUS threat. Overall strategic success depends upon a clear understanding and appreciation of our present vulnerabilities.

The United States national security strategy provides for two, nearly simultaneous, major regional contingency (MRC) operations.[1] The US deterrent policy relies on power projection and the ability to get forces to the MRC theater in a timely manner to achieve US strategic goals. By causing a delay in the US deployment plan, a belligerent power could steal the initiative and conclude the hostilities before the US could enter the conflict.

Two major studies have shaped US strategic mobility requirements: The Mobility Requirements Study (MRS) in 1992 and the Bottom-Up Review (BUR) in 1993.[2] The MRS was updated in March 1995.[3] These analyses of our strategic deployment requirements did not consider a CONUS threat and assumed that US port operations would occur without interruption.

Operations Desert Shield and Storm were the most intensive military deployments since World War II. More than 500,000 personnel and almost ten million tons of material were transported to Southwest Asia in a seven month period, without a serious incident at any CONUS port. The luxury of time to build up Allied forces was a critical factor in the successful outcome of the campaign. It would be a strategic error to assume that build-up time will be available in future conflicts and that our domestic ports will operate free from hostile disruptions.

An inordinate emphasis has been placed on examining US strategic mobility in the CINC's OCONUS area of responsibility. Approximately 95 percent of all supplies and equipment arrive in theater by sealift. Mobilization planners assume that US ports will remain open and free to meet the CINC's needs.

The changing world order has increased the proliferation of weapons of mass destruction and the ease with which they are obtained. Virtually no nation or institution is beyond the grasp of today's technologically advanced and well financed terrorist group.

The purpose of this paper is to demonstrate that our domestic sea ports and terminals, which deploy and sustain our armed forces, present a critical vulnerability which requires improved security measures. Given the vulnerability of the seaports, the real issue is to determine whether they are unnecessarily susceptible to extended disruption by sabotage or terrorist action. This is answered by determining the following: (1) what critical features exist at each port; (2) whether these have been afforded appropriate attention; and (3)

whether system recovery planning and redundancies exist in the event of a successful attack.

This analysis addresses only east coast strategic seaports and focuses on creating disruptions which would curtail operations for more than one week. As such, it allows a broad enough view to demonstrate the general vulnerabilities to all US ports. I will explain port security responsibilities, potential threats, existing security and countermeasures, critical features of a port, port specific vulnerabilities, consequences of disruption, recommendations, and conclusions.

## Responsibilities

Owners and operators of vessels or waterfront facilities have the primary responsibility for protecting and securing their property. They are required to take all necessary precautions for protection against sabotage and other subversive acts.[4]

In January 1985, six Federal agencies within DoD and the Department of Transportation (DoT) with responsibilities for port readiness signed a memorandum of understanding (MOU) that called for close coordination to assure rapid deployments for national defense. In September 1988, a seventh organization, the Maritime Defense Zone (MDZ), was added to the group. The MOU recommended the creation of a local Port Readiness Committees (PRC) to enlist multi-agency support of the overall program. The MOU also delineated responsibilities for port security.[5]

Port and terminal security is a shared responsibility among federal, state, and local governmental agencies as well as the

involvement of private businesses (see Appendix A). No one, single agency is the overall proponent for port and terminal security. Each of the agencies, individual businesses, and other interested participants provides input into issues involving security. The United States Coast Guard (USCG) is responsible for the waterside threat. The Military Traffic Management Command (MTMC) is responsible for those portions of terminal security associated with the military outload. The port authorities have security responsibilities associated with the port, terminals, and shipping. Never the less, there is not a single, unified proponent for port and terminal security.

## Threats

### General

Future threats to US interests will encompass the full spectrum of conventional and unconventional operations. Future conflicts can range from general war to operations other than war (OOTW). Advanced technologies have extended the dimensions of the battlefield. Future threats may emerge from within the US as well as from foreign sponsored acts of sabotage and terrorism against the US mainland. Consequently, the US can ill-afford to assume its historic complacence in port security.

Threats to domestic ports are initially identified by the intelligence community. The FBI is the lead agency in the identification and monitoring of acts of terrorism and sabotage. Inter-agency communication and coordination is vital to ensure that current intelligence summaries are disseminated to the federal, state, or local agency required to respond to the potential threat.

No one definition of terrorism has gained universal acceptance. Terrorism is officially defined by the FBI as, "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social goals".6 Sabotage refers to an act "with the intent to interfere with or obstruct the national defense by willfully injuring or destroying any national defense or war material, premises, or utilities including humans and natural resources".7

Types of Terrorist Organizations in the US

Ethnic separatist and emigre groups (ie. Puerto Rican nationalists (Armed Forces of National Liberation, FALN), Jewish extremists, Croatian, Haitian, etc.) seek to expand their political aims in the US and abroad. Generally, these groups do not support the US government's position in relation to their native country and use terrorism as a means to coerce the US to adopt a policy more favorable to their position.

Left-wing radical organizations (ie. May 19th Communist Organization (M19CO), United Freedom Front (UFF), etc.) are characterized by extreme egalitarianism, hatred of capitalism, and overt opposition to militarism. Recent leftist terror in the US is attributed to holdovers from the student movements and radical prison reforms of the 1970s.

Right-wing racist, anti-authority, survivalist, and other extremist groups (ie. Aryan Nations, Sheriff's Posse Comitatus (SPC), the Order, etc.) are characterized by a belief in the superiority of their race or national group and the desire to make their own group supreme over others.

Issue-oriented groups (ie. Earth First, Animal Liberation Front (ALF), etc.) address a broad spectrum of concerns, many of which are incompatible. To date, only environmentalists have resorted to acts of terrorism, frequently resorting to sabotaging construction and development projects.

The protected status of the US disappeared after the 1993 bombing of the World Trade Center. Ireland, Libya, Iran, Syria, Japanese Red Army (JRA), Abu Nidal, Sikhs, and others no longer shy away from acting on US soil. Virtually every anti-US, terrorist organization seeks to export terror to the US.

Many of these foreign terrorist organizations have support networks within the United States (ie. IRA, JRA, Shining Path, al-Fateh, Hamas, etc). Los Angeles street gangs have been accused of involvement with the Medellin Cartel, and members of the El Rukn gang in Chicago were convicted of conspiring with the Libyan government. "The most likely prospect is that terrorist episodes on US soil will become more common".[8]

Threat Capabilities

In 1983, four FALN leaders were indicted for bombing five military installations. In 1986, eight members of the UFF were indicted for bombing four Army and Navy Reserve centers. In 1989, five environmental extremists were indicted for conducting sabotage at a nuclear power station.[9] Libyan agents in Washington, DC in 1987, members of the Syrian Social Nationalist party in 1987, and Japanese Red Army members in 1988 were each captured before carrying out planned bombings in this country. In spite of the FBI's increased efforts, terrorist organizations continue to pose an increasingly more dangerous threat.

"Almost all violent extremist movements select two basic types of targets: those that help to fund their operations and those that help to further the political or social causes advocated by the organization."[10] Properly financed, any organization can obtain weapons, ammunition, explosives, etc. Additionally, these organizations can 'hire' the skills and services of others to assist them in carrying out their goals.

Extremist organizations use terrorist tactics to further their political or social aims. Recent train hijackings and derailments demonstrate the ease with which organized bands can attack US property with impunity.[11] Arson and bombing remain favorite tactics of extremist groups. Environmental extremists have proven the relative ease of infiltrating guarded areas to conduct industrial sabotage. In Japan, the JRA created a shock wave after waging a successful, lethal gas attack.

Attempts to close our borders have not deterred drug traffickers and illegal aliens from entering the US. Almost anyone or anything can be smuggled into the country. Virtually no institution or facility is beyond the grasp of a well-organized and financed extremist group bent on achieving their local objective.

Summary

There is no such thing as a common terrorist profile in the US. Terrorist organizations cover the gamut of motivations, causes, goals, and methods. The common feature is that they break the law and jeopardize the lives, liberties, and properties of American citizens. These criminals will target individuals, buildings, and properties to expand their aims.

An act of terrorism or sabotage tied to a military deployment could seriously affect the MRC plan. The US ports which deploy and sustain our armed forces present a vulnerable target whose damage or destruction would enhance the prestige of any terrorist organization as well as to seriously jeopardize the timely execution of the MRC plan.

## Vulnerability of Networks

### General

Vessels, facilities, and equipment are vulnerable if they are susceptible to damage and if an element can successfully attack and damage the target. No measure exists that can determine absolute vulnerability. The USCG, MTMC, port authorities, and others have vulnerability assessments and physical security checklists to provide a method for determining the relative vulnerability of port facilities. Factors which determine vulnerability include: geographical location; accessibility to the target (ingress and egress); the nature and construction of the target; the amount of damage required; resources required to destroy, damage, or steal the target; and, the adequacy of security forces and physical security measures.

"While the number of domestic maritime terrorist or subversive acts have been few, the vulnerability of many US ports is quite high."[12] All ports possess vulnerabilities based on two types of characteristics. The first type includes characteristics common to all port facilities (ie. access roads and railways, unobstructed channel, reliance on electricity, use of telecommunications and computers, use of piers and cranes, a waterside threat, an aerial threat, and a landside threat). The

second type includes port-specific characteristics which, if attacked and disabled, would degrade the port's ability to conduct deployment operations. This second includes a port-specific Achilles' heel (ie. a water choke point, key bridges, critical reliance on port infrastructure, etc.).

The National Port Readiness Network identifies strategic ports for military use. MTMC provides input based on the port's geographic location, facilities and capabilities. East coast strategic ports include: New York, NY; Bayonne, NJ; Hampton Roads, VA; Morehead City, NC; Sunny Point, NC; Wilmington, NC; Charleston, SC; Savannah, GA; and Jacksonville, FL.

All of the ports provide adequate facilities and berths to support a military outload (see Appendix B). Each state or local port authority provides security for the municipal terminals. The USCG has a designated Captain of the Port (COTP) for each port. MTMC designates a port commander for the terminal conducting the military outload.

Common Characteristics

A port consists of a harbor and the corresponding waterway which links it to a water transportation route. It extends to include the berths, docks, wharfs, piers, breakwater, sea wall and supporting waterfront facilities. A terminal is that part of a port consisting of the landside components required to support port operations. It extends to include the support buildings, staging areas, marshaling areas, warehouses, storage tanks, roads, railways, on-load/off-load equipment, and other components required to operate a port.

All harbors, ports, and terminals possess a degree of

vulnerability in our free and open society. Ports and harbors, in themselves, do not possess any vulnerable attributes. The only critical component of a port or harbor is that portion which lies within the restricted channel passage. On the other hand, berths, docks, wharfs, piers, sea walls, breakwaters, and waterside facilities are vital for port operations. However, the number of berths available in any port complex generally ensures that no single berth is critical to the overall port operation.

Terminals require specific facilities and equipment to maintain port operations. Roads, railways, electricity, telecommunications, cranes, material handling equipment, and support facilities provide the lifeline for port operations. Damaging or destroying a critical node would seriously disrupt port operations. Many ports have redundant systems or alternative sources available, thereby decreasing the criticality of any single component. Terminals without back-up plans are susceptible to extended disruptions and delays.

A common vulnerability to all ports is a mine threat. The USCG does not possess mine clearing capabilities and relies on US Navy assets to locate and clear mines. An adversary could merely claim that mines exist or actually deliver mines; the result would render the port incapable of ship traffic.

Another potential threat common to all ports involves railway movement to the port. Military shipments from home installations to ports of embarkation could be derailed at or near a port. The consequences, in terms of lost equipment and personnel could seriously impede the deployment schedule.

All ports and terminals possess certain common characteristics which are critical for their operations. However, most port authorities provide redundancy or have the ability to repair damage with limited disruption to the overall operation. Never the less, these common characteristics provide the basis for adversarial groups to begin planning acts of sabotage or terrorism against a port.

Port-Specific Characteristics

New York-New Jersey; Bayonne; and Hampton Roads: The single greatest threat to each of these ports rests with critical bridges. The Verrazano-Narrows Bridge, in New York, and the Hampton Roads Bridge Tunnel, in Virginia, lie within restricted channel passages. Collapsing a bridge or sinking a vessel at a choke point would create a bottleneck which would prevent port transit. Bridges present a clearly recognizable and relatively accessible potential target.

Waterway passage is a critical component of any port operation; creating an obstruction effectively halts operations until the wreckage is removed. Colonel Carmona (Commander, MTMC, 1302 Major Port Command) stated that an obstruction at one of these choke points could close the port for one to two weeks, until the channel is cleared.[13]

Morehead City and Wilmington: Both of these ports possess vulnerabilities associated with the railway support network. Each port is served with only one set of railroad tracks. The rail line serving Wilmington has a short section of single track at the northern approach to the port. Morehead City has 85 miles of single track from the switching station. Disabling

this single section of railroad track would inhibit the port's ability to outload a military unit. The railway presents a recognizable, accessible, and usually, unguarded target.

The rail network is a critical node for the port. Damage to the system would render the port useless. Chief Monroe (Chief of Wilmington Port Police) acknowledges these vulnerabilities and the impact on port operations. However, it is uncertain as to the extent and duration it would have on port operations.14

Sunny Point, NC: The Military Ocean Terminal, Sunny Point (MOTSU) is the only domestic DoD port for containerized ammunition. Detonating ammunition supplies could create collateral damage throughout the port and effectively curtail operations. Additionally, the port relies on a single railroad track from Leland (18 miles away). This isolated section of track is crucial for providing cargo to the port. Destroying the rail would prevent ammunition from arriving at the port. A third vulnerability is that MOTSU has only one berth which is capable of loading containerized ammunition; destroying this single, critical berth would devastate port operations. Additionally, MOTSU has only two container cranes and no back up system in the event of crane damage or loss.

MOTSU's cargo, rail, and single container berth constitute critical vulnerabilities to the port operation. A loss to any one component would prove disastrous. No other port is as critical for the successful accomplishment of an MRC scenario. The US has no comparable replacement for the functions provided by MOTSU. The loss or degradation of port operations could have serious ramifications on a warfighter's plan. MOTSU's targets

are identifiable and, with adequate planning and determination, accessible. Colonel Parker (Commander, MOTSU) acknowledges the devastating consequences of a successful attack against his facility and admits that it could take weeks to recover.[15]

Charleston, Savannah, and Jacksonville: All three of the ports possess critical vulnerabilities associated with bridges. All three ports are located upstream from bridges whose collapse would isolate the ports from the ocean.

The channels are critical for port operations. The bridges are recognizable and accessible. Colonel Brady (Commander, MTMC, 1304 Major Port Command) understands the vulnerability of the bridge networks and admits that it could take more than a week to clear the wreckage and reopen the channel.[16]

**Consequences of Disruptions**

Port operations are the vital link in the deployment process between the CONUS and intertheater flows. Without this bridge, the deployment flow ceases and results in a massive traffic jam of millions of square feet of cargo on thousands of rail cars, trucks, and organic vehicles from dozens of origins and hundreds of ships without the ability to connect.[17]

An act of sabotage or terrorism could strain relations between levels of government as well as with the local population. Business and industry may seek to deny the use of terminals to DoD, or increase the rates charged. Public outcry and concerns for safety could damage relations. Intermodal carriers (ie. truck, rail, barge, ship, air) could become difficult to procure if the fear of terrorism was substantiated.

Port throughput capacity must support the flow of cargo as

it arrives at the port. The entire deployment sequence is a carefully planned and executed process. Ports continue to receive additional outbound cargo as vessels are loaded and depart. Natural or manmade accidents would seriously jeopardize the entire deployment process. USTRANSCOM would have to hastily obtain additional railcars, trucks, berths, as well as reroute ships to accommodate for the loss of any one port.

The decrease in forward basing compels all services to rely on ports to move their equipment to the theater. Theater CINCs develop MRC plans based on required delivery dates (RDD). The consequences of a disruption at a port could delay equipment and supplies from arriving in theater when the CINC needs it.

**Countermeasures**

All of the strategic ports have active, full-time physical security measures. The USCG, port police, MTMC, and other agencies all have different definitions of physical security. Never the less, all are concerned with safeguarding personnel, preventing unauthorized access to equipment, material, documents, and safeguarding them against acts of espionage, sabotage, terrorism, damage, and theft.

Physical security standards vary from port to port. There is not a standardized format in use by all agencies. The USCG and US Army have physical security regulations and standard checklists. However, neither uses the other's forms and neither are universally accepted by all port authorities.

Many ports have federal, state, and local agencies who enforce regulations. Customs, Immigration, USDA, ATF, and other agencies maintain offices in many of the larger, international

ports. Their communication and cooperation enhances the security of the port.

Most of the inter-agency coordination which address security issues is conducted at an informal level. Formal interagency coordination often occurs far above the levels of those who are charged with executing actions. At these higher levels, security issues are seldom discussed until a crisis occurs.

The National Port Readiness Network (NPRN) reviews port security plans and coordinates with other agencies to ensure that all security requirements are addressed. The Port Readiness Committee (PRC) takes a lead role in planning local port operations in the event of a national emergency. The USCG, as the COTP, chairs these meetings and focuses on issues requiring immediate attention.

The USCG develops plans to address waterside security issues. The port police develop plans to address day-to-day, peacetime and crisis response operations. MTMC develops plans to address mobilization and deployment issues. While the goal is the same for all agencies, they seldom meet to discuss common security issues.

Security planning must determine where to focus limited port security resources. However, not everyone agrees as to which assets are at the greatest overall risk. Security planning and resource management must consider potential threats to assets in ports and how their destruction or damage might impact on port operations.

**Recommendations**

The NPRN should designate the USCG as the single proponent

for all aspects of security, during peace and times of national emergency. The COTP presently plays a lead role in security; his authority should extend to encompass landward security.

The FBI should improve its coordination and communication with the NPRN. The NPRN needs to develop a method for the dissemination and exchange of information to enhance port security procedures. This will enable agencies and operators to adjust their procedures in response to changing conditions and specific threats. The prompt, clear, and orderly dissemination of information is vital to the success of the security program.

The NPRN needs to adopt standard physical security checklists and port vulnerability assessments. The services should develop "Joint" doctrine for port operations, specifically in the area of physical security.

The State Area Command (STARC) of the Army National Guard (ARNG) should establish Port Security Companies (PSCs) for each strategic port within their state. In the event of national emergency, the Governor (and not the President) could call his/her troops to active duty. The states already acknowledge their responsibilities under the Key Asset Protection Program (KAPP); DoD should formalize their commitment to the security of the ports. This move would significantly enhance the security of our strategic ports.

Given the inherent vulnerability of the ports, additional research is needed to determine whether the risks warrant the costs associated with implementing improved security measures. Research is also warranted in the area of recovery planning.

## Conclusion

The proliferation of weapons of mass destruction and the relative ease with which they are obtained has increased the vulnerability of the US mainland. The recent bombings in Oklahoma City and of the World Trade Center demonstrate the vulnerability of the US to acts of terrorism. Terrorist threats to US ports are a potential reality which cannot be dismissed lightly. The threat may develop from internal, domestic organizations who are disaffected with the political situation. Foreign terrorist organizations are eager to export their campaigns to the US. The US ports present an exposed target whose attack would serve to enhance the aims of any terrorist organization.

In 1988, Oliver Revell, Executive Assistant Director for the FBI, told a Senate Subcommittee that, "it is unrealistic to assume that we have the ability or resources to guarantee protection to our nation's infrastructure from every conceivable terrorist attack."[18] The United States remains a free and open society. Virtually anyone can obtain weapons, explosives, and other materials to achieve terrorist aims. Although the use of terrorism has not significantly altered the course of past wars, it is conceivable that terrorists could hinder our ability to deploy and sustain our forces.

Theater CINCs develop plans based on the projected arrival of units and equipment. The successful MRC scenario is predicated on the ability of US strategic mobility assets arriving in accordance with the programmed schedule. Service Chiefs and Theater CINCs depend on port throughput to deploy and

sustain our forces. The possibility that a single, violent act can shatter the balanced, time-sensitive US deployment schedule demands a new sense of awareness and vigilance on the part of DoD. Port security is a vital aspect of the mobilization, deployment, and sustainment process.

The ability to fight and win is dependent on the effectiveness with which US forces are projected into any theater of conflict. History has demonstrated the critical role our ports play in supplying a credible deterrent force. The goal of future mobility planning must ensure that our ports remain open and unencumbered in providing forces whenever and wherever needed.

## End Notes

1. A National Security Strategy of Engagement and Enlargement, (Washington: The White House, 1995), 9.

2. U.S. Department of Defense, Report of the Bottom-Up Review, (Washington: 1993), 1-109.

3. U.S. Department of Defense, Joint Chiefs of Staff, Mobility Requirements Study, Bottom-Up Review Update, (Washington: 1995), 1-9.

4. "Protection and Security of Vessels, Harbors, and Waterfront Facilities," Code of Federal Regulations, Title 33--Navigation and Navigable Waters, (Washington: U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, 1 July 1995), chap. I, 70.

5. U.S. Department of Transportation, Maritime Administration, Port Emergency Operations Handbook for Federal Port Controllers, (Washington: 1992), Appendix E.

6. U.S. Department of Justice, FBI Terrorist Research and Analysis Center, Terrorism in the U.S.: 1990, (Washington: 1991), 25.

7. U.S. Department of Defense, U.S. Special Operations Command, U.S. Special Operations Forces Posture Statement, (Washington: 1994), D-4.

8. Institute for National Strategic Studies, Strategic Assessment, 1995, (Washington: 1995), 176.

9. Brent L. Smith, Terrorism in America: Pipe Bombs and Pipe Dreams, (New York: SUNY Press, 1994), 17-29.

10. Ibid., 43.

11. "Border Bandits," CBS Evening News (Television Broadcast), 29 May 1995, S. Pelley.

12. U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 2-3.

13. Telephone conversation with Colonel Carmona, Commander, MTMC, 1302 Major Port Command, Bayonne, NJ, 17 January 1996.

14. Telephone conversation with Chief Monroe, Chief of Wilmington Port Police, Wilmington, NC, 8 January 1996.

15. Telephone conversation with Colonel Parker, Commander, MTMC, 1303 Major Port Command, Sunny Point, NC, 26 January 1996.

16. Telephone conversation with Colonel Brady, Commander, MTMC, 1304 Major Port Command, Charleston, SC, 29 January 1996.

17. U.S. Department of Defense, Joint Chiefs of Staff, Mobility Requirements Study, Bottom-Up Review Update, (Washington: 1995), E-I-6.

18. Oliver B. Revell, III, "Statement", U.S. Congress, Senate Committee on Judiciary, Terrorist Attacks Against the United States, Hearings, (Washington: U.S. Govt. Print. Off., 1990), 5.

## Appendix A

### Responsibilities

Department of Transportation (DoT)

DoT is responsible for all aspects of the nation's transportation system. It interacts with other agencies in carrying out national security policies. It also provides law enforcement and traffic management services for the nation's airspace and waterways.

The Office of Emergency Transportation (OET) is responsible for developing the overall DoT emergency preparedness policies, plans, and programs, as well as ensuring the effective integration of the civil emergency preparedness programs of all elements of the federal transportation community. OET works closely with DoD to provide civil transportation service in support of national mobilization and deployment objectives.

Maritime Administration

MARAD (an agency within DoT) is responsible for proper operations of US seaports under national emergency conditions. MARAD accomplishes this by implementing plans through the National Shipping Authority, the Federal Port Controller network, and the National Port Readiness Network.

United States Coast Guard (USCG)

The U.S. Coast Guard is responsible for the security of all U.S. ports. The Coast Guard is tasked to develop emergency response plans both as a federal law enforcement agency and as a military service to meet national mobilization requirements.

The USCG assigns a senior officer as the Captain of the Port (COTP) for each major US port. The COTP has overall

responsibility for ensuring that adequate security is maintained to safeguard vessels, waterfront facilities, and harbors within his/her jurisdiction. The COTP identifies critical assets within a port, develops a prioritized list of those most susceptible to acts of sabotage, and plans adequate security measures to meet specific needs. Additionally, the COTP is responsible for providing waterside security for essential port facilities and maritime assets. Landside security, particularly as it pertains to landward approaches to facility property, falls primarily to the owner/operator of the vessel or facility and state and municipal law enforcement agencies.

Department of Defense (DoD)

The Assistant Deputy Undersecretary of Defense for Transportation Policy (ADUSD(TP)) is responsible for oversight of all transportation matters within DoD. Policy responsibility encompasses all aspects of the transportation system using all organic and contracted transportation services.

DoD is prohibited by law from exercising most civilian law enforcement powers by 18 USC 1385. DoD has primary responsibility for protecting its own facilities. This authority extends to waters which are exclusively under the control of DoD.

Maritime Defense Zones (MDZ)

MDZs are USN Third Echelon commands within the fleet CINC organization. In peacetime, MDZ commanders are responsible for planning and exercising Naval Coastal Warfare (NCW). When activated, they become operational commanders responsible for NCW within the MDZ area of responsibility (AOR). The commanders

prescribe overall tactics, allocate assigned resources to meet threats, and maintain overall command within their AOR.

US Transportation Command (USTRANSCOM)

USTRANSCOM is a combatant command responsible for coordinating and ensuring all mobility requirements are met in support of the national security strategy.

Military Sealift Command (MSC)

MSC, as a component of USTRANSCOM, provides strategic sealift for the support and sustainment of military forces wherever needed. MSC relies on its Strategic Sealift Force of government-owned and chartered US flag ships.

MSC relies on three operational strategies to provide rapid and continuous military support. They include prepositioning, surge, and sustainment sealift. Prepositioning provides the necessary logistical support already loaded aboard ships which are strategically located near potential crisis areas. Surge shipping involves the transport of large, bulky military equipment (ie. tanks, trucks, helicopters, etc.) needed quickly on site during a war or contingency. Sustainment shipping follows to keep the supply-line flowing with the armament, food, and other items necessary for continued presence overseas.

Military Traffic Management Command (MTMC)

MTMC is the component of USTRANSCOM which coordinates force movement to seaports, prepares the ports for ships and cargo, and supervises the loading and offloading operations at ports. MTMC designates a major port command (MPC) to plan, coordinate, and control MTMC operations at each strategic port. MTMC relies on augmentation from the Reserve Component to operate ports and

terminals in times of national emergency.

Transportation Terminal Brigade/Battalion (TTB)

A TTB is designated to manage military traffic operations at a port. The TTB plans, arranges, and supervises the loading of military equipment and cargo on ships. The TTB commander is normally the Port Commander of the military port. Presently, all 18 TTBs are in the Army Reserve.

Port Security Company (PSC)

A PSC provides physical security for the military operation of a port during loading operations. The PSC controls access to port areas, mans traffic control points, patrols rail and wharf areas, inspects vehicles, escorts convoys, and guards equipment and sensitive cargo. A PSC works with other security elements, including the USCG, local police, and other military elements. Presently, all three PSCs are in the Army Reserve.

Federal Bureau of Investigation (FBI)

The FBI is charged with investigating all violations of federal law with the exception of those that have been specifically assigned by statute to some other federal agency. The FBI's jurisdiction includes espionage, sabotage, terrorism, and other domestic security matters. The FBI is the designated lead agency for response to domestic maritime terrorist incidents.

Port Readiness Committee (PRC)

At each strategic port, representatives of the seven MOU Port Readiness Signatory Agencies establish a port readiness committee. The PRC coordinates peacetime preparations for port operations in emergencies. In addition to the seven members,

the PRC includes businesses, port authorities, and other interested participants. For consistency, the USCG chairs each local PRC.

Other Agencies

The security and defense of the nation's ports involves numerous organizations which are responsible for different aspects of port safety, security and harbor defense.

Federal agencies (ie. Customs, USDA, INS, etc.) have officials at the ports to enforce the laws under their purview.

State and local law enforcement agencies generally deal with crimes against real property and persons (ie. trespass, breaking and entering, disturbing the peace, assault, etc.). These agencies generally have jurisdiction on land. In some areas, however, agencies have been established that have full law enforcement authority for all waters within their jurisdiction (ie. harbor masters and harbor police).

Intentionally Blank.

## Appendix B

### Strategic Ports

New York, NY The Port of New York-New Jersey consists of several terminals, all of which are located north of the Verrazano-Narrows Bridge. The port condition varies from antiquated and deteriorating berths to modern facilities. The port complex has more than 100 berths, exceeding 40,000 linear feet, and is capable of day/night operations.

A 7-foot chain link fence topped with barbed wire encloses each terminal. Each terminal provides security for its own respective area. NY-NJ Port Police control gates and conduct patrols 24 hours a day. Lighting further enhances security of the port.

Bayonne, NJ Although located within the NY-NJ port district, the Military Ocean Terminal Bayonne (MOTBY) is a separate entity. MOTBY is a manmade, timber pile pier with a timber-decked platform. It has 19 berths totaling 11,083 linear feet, is well lighted and capable of day/night operations.

A seven foot chain link fence topped with barbed wire encloses the terminal. Cargo staging areas within MOTBY are also secured with additional fencing. DoD police provide 24 hour security, controlling gate access and conducting patrols. The terminal's perimeter is well lighted, as are the berths, staging, and open areas.

Hampton Roads, VA The Port of Hampton Roads is located in southeastern Virginia at the southwest corner of the Chesapeake Bay. Norfolk and Portsmouth facilities are located on the south side, Newport News terminal on the north side. Wharf

construction is a composite of timber pile, concrete, and steel. The terminals capable of supporting military outload, have 30 berths, totaling 21,745 linear feet and are can support day/night operations.

A chain link fence encloses each of the terminals. Virginia Port Authority police provide 24 hour gate and patrol services. Lamberts Point Dock provides its own private security guards.

Morehead City, NC The Port of Morehead City is located on the tip of a peninsula about 100 miles northeast of Wilmington, NC. Fort Bragg is 140 miles west, Camp Lejeune is 45 miles west, and Cherry Point is 20 miles west. The port has nine berths totaling 5,050 linear feet. The bulkhead is concrete capped/steel sheet piling. The port presently does not own large mobile cranes. Lighting is available for night operations.

An unlighted, seven foot chain link fence, topped with barbed wire encloses the port. A small detachment from the North Carolina State Port Police provides 24-hour gate and patrol security.

Sunny Point, NC The Military Ocean Terminal at Sunny Point (MOTSU) is about 100 miles southwest of Morehead City, NC. It occupies a terminal on the west side of the Cape Fear River. The bulkhead is concrete capped/steel sheet piling. MOTSU is the only existing facility for containerized ammunition. It has 6 berths and is capable of day/night operations.

A seven foot chain link fence topped with barbed wire encloses the terminal. DoD police provide 24 hour protection, control gate access and conduct patrols. DoD police also provide 24

hour waterside security with a patrol boat.

Wilmington, NC The Port of Wilmington is 170 miles northeast of Charleston, SC. The port has 11 berths totaling 6,742 linear feet. Wharf construction is concrete piling with a concrete apron and rubber fender system. It is capable of day/night operations.

A six foot chain link fence topped with barbed wire encloses the terminal. Some areas of the perimeter do not have lighting. The North Carolina State Port Police provide 24-hour patrol services and gate security.

Charleston, SC The Port of Charleston is 102 miles northeast of Savannah, GA. Two terminals are near downtown Charleston. A third terminal is eight miles up the Cooper River and houses MTMC's 1304 Major Port Command at the US Naval Weapons Station. A fourth major terminal is five miles northwest on the lower reach of the Wando River. The wharfs vary in age, construction, and condition at each of the terminals. The four terminals provide 15 berths totaling more than 12,328 linear feet and are capable of day/night operations.

A seven foot chain link fence topped with barbed wire encloses each terminal. The South Carolina State Police provides security guards and patrols. Also, an automated monitoring system provides additional security and detects fires. DoD police provide security at the USN Weapons Station and pier.

Savannah, GA The Port of Savannah is on the Savannah River in southeast Georgia. Its two main facilities are located on the south bank of the river. Most berths are open wharf, with concrete piling and aprons. The port has 17 berths totaling

12,288 linear feet and is capable of day/night operations.

Chain link fencing encloses each terminal, except at rail access points. All gates are controlled 24 hours a day by Georgia Port Authority Police. A security and fire protection unit patrols each terminal 24 hours a day.

Jacksonville, FL The Port of Jacksonville is located on the St. Johns River, 345 miles north of Miami, Florida. The port has two main terminals providing eleven berths totaling 7,600 linear feet and is capable of day/night operations. Dock structure typically consists of concrete pilings and aprons.

An eight foot chain link fence topped with barbed wire encloses the Talleyrand Terminal perimeter. The Blount Island Terminal does not have perimeter fencing because the highway and rail bridges restrict land access. The Jacksonville Port Authority provides security guards to control access and patrol the terminals 24 hours per day.

## Selected Bibliography


A National Security Strategy of Engagement and Enlargement. Washington: The White House. 1995.

Bellin, David and Gary Chapman. Computers in Battle, Will They Work?. Boston: Harcourt, Brace, and Jovanivich, 1987.

"Border Bandits." CBS Evening News (Television Broadcast). 9 May 1995. S. Pelley.

Bowman, Stephen. When the Eagle Screams: America's Vulnerability to Terrorism. New York: Carol Pub., 1994.

Code of Federal Regulations, Title 33--Navigation and Navigable Waters. Washington: U.S. General Services Administration. National Archives and Records Service. Office of the Federal Register. 1 July 1995.

Computers: Crimes, Clues, and Controls. US Federal Document. Washington: CSIS, 1991.

Davies, D.W. and W.L. Price. Security for Computer Networks. New York: John Wiley and Sons, Inc., 1984.

Hafner, Katie and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon and Schuster, 1991.

Harvey, Robert N. "The Port Authority of NY and NJ's Organizational Strategy for Recovering The World Trade Center After the Feb 26, 1993 Terrorist Bombing." Cost Engineering. 10 January 1995. 35-37.

Hoffman, Bruce. Responding to Terrorism Across the Technological Spectrum. Santa Monica, CA: Rand, 1994.

Institute for National Strategic Studies. Strategic Assessment, 1995. Washington: 1995.

Riley, Kevin and Bruce Hoffman. Domestic Terrorism: A National Assessment of State and Local Preparedness. LC 94-47133. Santa Monica, CA: Rand, 1995.

Simon, Jeffrey. The Terrorist Trap: America's Experience with Terrorism. Bloomington, IN: Indiana Univ. Press, 1994.

Smith, Brent L. Terrorism in America: Pipe Bombs and Pipe Dreams. New York: SUNY Press, 1994.

Telephone conversation with Chief Monroe, Chief of Wilmington Port Police, Wilmington, NC. 8 January 1996.

Telephone conversation with Colonel Brady, Commander, MTMC, 1304 Major Port Command, Charleston, SC. 29 January 1996.

Telephone conversation with Colonel Carmona, Commander, MTMC, 1302 Major Port Command, Bayonne, NJ. 17 January 1996.

Telephone conversation with Colonel Parker, Commander, MTMC, 1303 Major Port Command, Sunny Point, NC. 26 January 1996.

U.S. Army. Ports for National Defense. MTMCTEA Report SE 90-3d-21. Military Traffic Management Command. Transportation Engineering Agency. Washington: 1992.

U.S. Congress. House. Committee on Appropriations. Departments of Commerce, Justice, State, the Judiciary, and Related Agencies Appropriations for 1995. Hearings. Washington: U.S. Govt. Print Offc., 1994.

U.S. Congress. House. Committee on Judiciary. The Future of U.S. Anti-Terrorism Policy. Hearings. Washington: U.S. Govt. Print. Offc., 1993.

U.S. Congress. Senate. Hearings Before the Senate Subcommittee on Terrorism and America. Hearings. Washington: U.S. Govt. Print. Offc., 1993.

U.S. Congress. Senate. Committee on Judiciary. Terrorist Attacks Against the United States. Hearings. Washington: U.S. Govt. Print. Off., 1990.

U.S. Congress. Senate. United Nations Convention on the Law of the Sea. Message from the President. Washington: U.S. Govt. Print Offc., 1993.

U.S. Department of Defense. Joint Chiefs of Staff. Mobility Requirements Study, Bottom-Up Review Update. Washington: 1995.

U.S. Department of Defense. Report of the Bottom-Up Review. Washington: 1993.

U.S. Department of Defense. U.S. Special Operations Command. U.S. Special Operations Forces Posture Statement. Washington: 1994.

U.S. Department of Justice. FBI Terrorist Research and Analysis Center. Terrorism in the U.S.: 1990. Washington: 1991.

U.S. Department of Justice. Federal Bureau of Investigation. Terrorism in the United States 1982-1992. Washington: 1993.

U.S. Department of Transportation. Maritime Administration. Port Emergency Operations Handbook for Federal Port Controllers. Washington: 1992.

U.S. Department of Transportation. Research and Special Studies Programs Administration. Port Needs Study: Study Overview. Washington: 1991.

U.S. Department of Transportation. United States Coast Guard. Marine Safety Manual; Volume VII, Port Security. COMDTINST M 16000.12. Washington: 1993.

Victor, Kirk. "Maritime Minefield: The Nation's Ailing Merchant Marine Needs Some First Aid." National Journal. 15 August 1992, 85-88.